REMARKS

In the Final Office Action, the Examiner rejected claims 1, 2, 4, 5, 7, 9-15, 17-37, 39-45, 47-66, 68, 69, 71-73, 75-90, and 138-157 under 35 U.S.C. § 103(a) as unpatentable over U.S. Patent No. 5,949,877 to Traw et al. ("*Traw*") in view of U.S. Patent No. 7,006,995 to Edenson et al. ("*Edenson*").

I. The Finality of the Office Action is Improper

MPEP § 707.07(f) states, "[w]here the applicant traverses any rejection, the examiner should, if he or she repeats the rejection, take note of the applicant's argument and answer the substance of it" (emphasis added). As set forth below, the Final Office Action does not comply with MPEP § 707.07(f).

In an Office Action mailed November 28, 2008, the Examiner rejected the claims of this application under 35 U.S.C. § 102(b) as allegedly anticipated by *Traw*. Applicants filed a Reply to Office Action on January 27, 2009 ("the Reply"), separately traversing the application of *Traw* to dependent claims 10, 24, and 33 (Reply at pages 45-46). Applicants pointed out distinguishing features of each of these claims on pages 45-46 of the Reply.

The final Office Action does not address Applicants' arguments regarding the applicability of *Traw* to dependent claims 10, 24, and 33. Instead, the final Office Action merely states that Applicants' arguments "have been considered but are moot in view of the new grounds of rejection" (Final Office Action at page 2). However, the Final Office Action does not rely on the newly cited *Edenson* reference in addressing these dependent claims, but rather continues to rely on *Traw* in addressing dependent claims 10, 24, and 33 (See Final Office Action at pages 5, 9, and 11).

Despite Applicants' traversal of these dependent claims in the Reply, the Final Office Action repeats precisely the same language in addressing dependent claims 10, 24, and 33 as was used in the non-final Office Action. For example, page 5 of the Final Office Action addresses dependent claim 10 and is identical to the language used to address claim 10 on page 4 of the non-final Office Action. Similarly, page 9 of the Final

Office Action addresses claim 24 with the same language as used in the non-final Office Action at page 8, and page 11 of the Final Office Action addresses claim 33 with the same language used on page 10 of the non-final Office Action.

As discussed above, the final Office Action simply dismisses Applicants' arguments regarding dependent claims 10, 24, and 33 without addressing them. Accordingly, the final Office Action improperly fails to address the substance of Applicants' arguments as required by MPEP § 707.07(f). Applicants were entitled to have their position regarding dependent claims 10, 24, and 33 addressed during open prosecution, and the finality of the Office Action is improper.

For the reasons discussed above, Applicants respectfully request that the Examiner reopen prosecution and consider Applicants' position with respect to these dependent claims, as required by the MPEP.

II. The Rejection of the Claims Under 35 U.S.C. § 103(a)

Applicants respectfully request that the Examiner reconsider and withdraw the rejection of claims 1, 2, 4, 5, 7, 9-15, 17-37, 39-45, 47-66, 68, 69, 71-73, 75-90, and 138-157 under 35 U.S.C. § 103(a). No *prima facie* case of obviousness has been established.

Independent claim 1 recites a data transmitting system comprising "[a] portable optical disc medium including ... a security module ... which executes a mutual authentication protocol with the drive unit" (emphasis added).

Traw discloses a method for protecting digital content by distributing a "Certificate Revocation List" (CRL) from a license authority to various devices (*Traw*, col. 5, lines 37-42). *Traw* discloses several methods of distributing the CRL, such transmitting the CRL over an IEEE 1394 bus between separate devices CRL (*Traw*, col. 3, lines 25-34), or including the CRL on compliant media that can also be used to distribute the CRL (*Traw*, col. 6, lines 48-52).

However, *Traw* does not disclose incorporating a security module into the compliant media. Instead, *Traw* merely discloses that the CRL is prerecorded on the

media, and compliant devices can update their CRL by reading the CRL from the media (*Traw*, col. 6, lines 48-52). Thus, *Traw's* CRL is embodied on conventional media and is simply read directly from the media. *Traw's* media lacks a security module or other device capable of executing a mutual authentication protocol. Accordingly, *Traw* does not teach or suggest "[a] portable optical disc medium including ... a security module ... which executes a mutual authentication protocol with the drive unit," as recited by independent claim 1 (emphasis added).

Edenson fails to cure these deficiencies of *Traw*. Edensen discloses an identification system module embedded in a digital storage media (*Edenson*, abstract and col. 6, lines 60-62). Edensen also discloses a media player that includes an interrogator that reads authorization data from the identification module (*Edenson*, ¶ 60-62). If the authorization data read from the identification system module matches the serial number of the media player, the media player will read the digital storage media (*Edenson*, col. 6, lines 60-67).

However, *Edenson* does not disclose or suggest any mutual authentication protocol that occurs between the interrogator and the identification system. Indeed, *Edenson* fails to even disclose or suggest that any information is transmitted from the interrogator to the identification module. Rather, like *Traw's* conventional media, *Edenson's* identification system is simply read to obtain data included therein. Accordingly, *Edenson* also does not teach or suggest "[a] portable optical disc medium including ... a security module ... which executes a mutual authentication protocol with the drive unit," as recited by independent claim 1 (emphasis added).

Although of different scope, independent claims 34 and 64 distinguish over the four cited references for at least the same reasons as claim 1. Claims 2, 4, 5, 7, 9-15, 17-33, and 138-145 depend from claim 1, claims 35-37, 39-45, 47-63, and 146-153 depend from claim 34, and claims 65, 66, 68, 69, 71-73, 75-90, and 154-157 depend from claim 64.

Moreover, as discussed above, dependent claims 10, 24, and 33 are further distinguishable from *Traw* for at least the reasons set forth on pages 45-46 of the Reply

As the Final Office Action continues to rely on *Traw* in addressing these dependent claims, Applicants respectfully refer the Examiner to these pages of the Reply. However, these dependent claims are also distinguishable from *Edenson*. Applicants will only provide remarks distinguishing dependent claim 33 from the cited art. With respect to claims 10 and 24, Applicants simply note that the Final Office Action relies on *Traw*, and not *Edenson*, in addressing these claims.

Claim 33 recites a system wherein "the security module reads data encrypted and stored in the portable optical disc medium, decrypts the encrypted data with the content key, re-encrypts the decrypted data with a shared key and sends the re-encrypted data to the drive unit" (emphasis added). As discussed in more detail on page 46 of the Reply, while *Traw* discloses using media to distribute a Certificate Revocation List ("CRL"), *Traw* does not disclose or suggest that the media perform any encryption processing. Indeed, as discussed, *Traw* merely discloses conventional media that do not include a security module or other device capable of performing encryption. Accordingly, *Traw* does not teach or suggest the claimed "security module reads data encrypted and stored in the portable optical disc medium, decrypts the encrypted data with the content key, re-encrypts the decrypted data with a shared key and sends the re-encrypted data to the drive unit" (emphasis added), as recited by dependent claim 33.

As discussed above, *Edenson* discloses a media player that includes an interrogator that reads authorization data from the identification module (*Edenson*, ¶ 60-62). However, *Edenson's* security module does not perform any encryption processing. Rather, *Edenson's* security module simply stores the authorization data (*Edenson*, col. 6, lines 60-67). Accordingly, *Edenson* also does not teach or suggest the claimed "security module reads data encrypted and stored in the portable optical disc medium, decrypts the encrypted data with the content key, re-encrypts the decrypted data with a shared key and sends the re-encrypted data to the drive unit" (emphasis added), as recited by dependent claim 33.

III. Conclusion

In view of the foregoing amendments and remarks, Applicants respectfully request reconsideration of this application and the timely allowance of the pending claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: July 13, 2009

By: /David W. Hill/
David W. Hill
Reg. No. 28,220